



Testimony of the Michigan Chemistry Council
before the Michigan House Criminal Justice Committee
Tuesday, November 3rd, 2015

Mr. Chairman and Members of the Committee,

My name is John Dulmes, and I'm the executive director of the Michigan Chemistry Council. On behalf of my members, thank you for the opportunity to provide testimony on the issue of drone security and the chemical industry.

Chemistry is our state's third-largest manufacturing sector, and our companies support nearly 120,000 Michigan jobs and generate \$127 million in state and local taxes. 96% of all manufactured goods are directly touched by the business of chemistry, making our industry essential to every facet of Michigan's economy.

Like many other industries, we are excited about the many beneficial applications of unmanned aircraft systems (UAS), or drones. These possibilities include:

- Plant/process equipment monitoring/inspections
- Environmental and safety inspections, including flare stack monitoring
- Infrastructure inspections, including remote fence lines and property boundaries
- Security surveillance, including perimeter security and access control
- Aerial photography and advanced imaging
- Emergency response operations, including incident, disaster, and spill response

While drone technology is promising, it also raises a number of questions and concerns, particularly about potential security threats. Along with refineries, power plants, and water treatment facilities, chemical facilities are generally recognized as a crucial part of the nation's critical infrastructure. Of course, our industry is committed to the safety of our employees and the communities in which we operate, and chemical companies nationwide have invested more than \$14 billion to enhance physical site, transportation, and cyber security at their facilities under the ACC's Responsible Care initiative. Many of our members are additionally regulated under the Department of Homeland Security's Chemical Facility Anti-Terrorism Standards (CFATS).

As the federal government and states consider further drone regulations, we feel it is necessary to ensure that sufficient protections are in place to prohibit the intentional misuse of drones over chemical facilities. We have provided you with a copy of language modeled after legislation enacted in Louisiana and several other states. This language would prohibit the intentional over-flight or surveilling of a critical infrastructure facility, or unauthorized distribution of such information. It would provide additional protection from possible dangers to our facilities. As an example, drones that malfunction over a chemical plant could fall into an active chemical process unit and create a safety hazard. Furthermore, drones could capture videos or photos of a chemical plant layout, revealing sensitive security information that could be later used for deliberate harm. In a worst-case scenario, drones themselves could be used as direct weapons against chemical plants. While our member companies have done much to ensure the safety and security of their facilities, drones unfortunately present a multitude of unpredictable concerns.

We understand this is an emerging area with many considerations, and we greatly appreciate the opportunity to share our perspective. We look forward to working with you on our suggested language.

Drone Bill – Based on LA HB 1029 (Effective 8/1/14)

DRAFT

§X. Unlawful use of an unmanned aircraft system

A. Unlawful use of an unmanned aircraft system is:

- (1) the intentional over flight of a designated facility by an unmanned aircraft system without the prior written consent of the owner of the designated facility;
- (2) the intentional use of an unmanned aircraft system to conduct surveillance of, gather evidence or collect information about, or photographically or electronically record a designated facility without the prior written consent of the owner of the designated facility; or,
- (3) the intentional distribution, posting or sharing of any kind of information, including audio, video or photographic recordings obtained through the unlawful use of an unmanned aircraft system without the prior written consent of the owner of the designated facility.

B. As used in this Section, the following definitions shall apply:

(1) "Unmanned aircraft system" means an unmanned, powered aircraft that does not carry a human operator, can be autonomous or remotely piloted or operated, and can be expendable or recoverable. "Unmanned aircraft system" does not include any of the following:

(a) A satellite orbiting the earth.

(b) An unmanned aircraft system used by the federal government or a person who is acting pursuant to contract with the federal government to conduct surveillance of specific activities for law enforcement purposes based on a reasonable suspicion that the surveillance is necessary to prevent imminent danger to health, safety or the environment.

(c) An unmanned aircraft system used by the state government or a person who is acting pursuant to a contract with the state government to conduct surveillance of specific activities for law enforcement purposes based on a reasonable suspicion that the surveillance is necessary to prevent imminent danger to health, safety or the environment.

(d) An unmanned aircraft system used by a local government or a person who is acting pursuant to a contract with the local government to conduct surveillance of specific activities for law enforcement purposes based on a reasonable suspicion that the surveillance is necessary to prevent imminent danger to health, safety or the environment. (2)

"Designated facility" means the following systems:

(a) Petroleum refineries.

(b) Chemical and rubber manufacturing facilities.

(c) Petroleum or chemical storage facilities

(d) Electric generation facilities.

(f) Rail yard facilities.

(g) Commercial port and harbor facilities.

(h) Drinking water treatment facilities.

(3) "Federal government" means the United States of America and any department, agency, or instrumentality thereof.

(4) "State government" means the state of XXXXXX and any department, agency, or instrumentality thereof.

C.(1) Nothing in this Section shall prohibit a person from using an unmanned aircraft system to conduct surveillance of, gather evidence or collect information about, or photographically or electronically record his own property, or distribute, post or share such information that is either of the following:

(a) Located on his own immovable property.

(b) Located on immovable property owned by another under a valid lease, servitude, right-of-way, right of use, permit, license, or other right.

(2) Third persons retained by the owner of the property described in Paragraph (1) of this Subsection shall not be prohibited under this Section from using an unmanned aircraft system to conduct activities described in Paragraph (1) of this Subsection.

(3) Nothing in this section shall prohibit a person from lawful use of an unmanned aircraft system including for recreational or hobby purposes.

D. The provisions of this Section shall apply unless preempted by applicable federal law or by regulations adopted by the Federal Aviation Administration.

E.(1) Whoever commits the crime of unlawful use of an unmanned aircraft system shall be fined not more than five hundred dollars, or imprisoned for not more than six months, or both.

(2) On a conviction for a second or subsequent offense, the offender shall be fined not less than five hundred dollars nor more than two thousand dollars, or imprisoned for not less than six months nor more than one year, or both.

(3) Any designated facility aggrieved by the unlawful use of an unmanned aircraft system may initiate a civil action against the offending party to obtain all appropriate relief in order to prevent, restrain or compensate a violation of this section.

F. If any provision of this act or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of the act that can be given effect without the invalid provision or application, and to this end the provisions of this act are severable.

G. This act shall take effect immediately.

CHEMICAL PROCESSING

LEADERSHIP | EXPERTISE | INNOVATION

LOGIN | REGISTER



MENU

[Home](#) / [Articles](#) / [2015](#) / [Plant Security Is Now Up in the Air](#)

Plant Security Is Now Up in the Air

The proliferation of low-cost drones raises issues industry should confront.

By Mark Rosenzweig, Editor in Chief

Aug 12, 2015

[Print](#)[Email](#)[Tweet](#)[Share](#)[G+](#)[Share](#)

The sign at the gatehouse states in big bold red letters: "Photography prohibited anywhere within the plant." In addition, each visitor is escorted to a room in the administration building to see a safety video that ends with "Taking photographs while on this site is not allowed." Then, someone from the plant asks for the visitor's smartphone or camera, noting that the devices will be returned when the visitor's badge is turned in. And this is only after potential visitors — long before entering the plant gate — have undergone basic screening to see if they should be permitted on site in the first place.

Call them prudent or paranoid, such steps are increasingly common. The lawyers and security teams at many companies consider them essential. After all, the location, size and shape of equipment and other such details may reveal proprietary technology, the number and nature of railcars on site may offer commercial insights, and both types of information may enable potential attackers to discover vulnerabilities.

However, the adequacy of such measures increasingly is up in the air — quite literally. The emergence of relatively low cost and more capable drones is adding a new dimension to safeguarding intellectual property and protecting plant assets and personnel. Drones already provide high-resolution surveillance photos and real-time video; work now is underway to use them to deliver goods, from getting emergency medical supplies to hard-to-reach locations to speeding receipt of your latest

"Adapting the machines to nefarious purposes isn't much of a stretch."

purchase from an online retailer. And, indeed, process plants eventually may benefit from such capacities, e.g., to capture the current configuration of units to update drawings, to supply live feeds of the condition of remote equipment, and to quickly transport needed parts and tools. However, adapting the machines to nefarious purposes isn't much of a stretch.

Yet, this is an issue that seems to have flown below the radar at most plants.

Sure, helicopters and light planes already can fly over sites to collect information — and could be used to cause damage or worse. It's a rare plant today that documents, let alone investigates, any aircraft that seems to be taking a particular interest in the site. I bet most facilities ignore these flyovers or casually dismiss them as likely from a regulatory body.

Such aircraft are relatively expensive, must display identification numbers prominently and generally take off and land at prescribed locations. This limits the risk to some extent and eases ongoing tracking of individual helicopters and planes but certainly doesn't rule out someone renting or hijacking an aircraft to spy on or sabotage sites.

Drones raise far greater potential concerns. They are becoming less and less expensive. Some units aimed at commercial applications now cost under \$2,000 and a hobbyist can buy a decent drone for about \$1,000. In the U.S., sales are unregulated.

The Federal Aviation Administration (FAA) is working on rules for the commercial use of drones at low altitudes. Its proposal would allow daylight flights of drones weighing 55 lb. or less so long as the devices stay at an altitude below 500 ft and fly slower than 100 mph. Drone operators would have to pass a test and get cleared by the Transportation Security Administration. However, these strictures wouldn't apply to hobbyists. The FAA now limits flights of hobbyist drones to an altitude less than 400 feet and within sight of the operator.

Clearly the number of drones in our skies will increase vastly in the coming years. So, we now should evaluate and address the potential threats to intellectual property and security they pose, rather than ignoring them and risking learning some hard lessons.



MARK ROSENZWEIG is Chemical Processing's Editor in Chief. You can email him at mrosenzweig@putman.net.

Join the discussion

We welcome your thoughtful comments. Please comply with our [Community rules](#). All comments will display your user name.

Want to participate in the discussion?

[REGISTER FOR FREE](#)

[Log in](#) for complete access.

Comments

No one has commented on this page yet.

[RSS feed for comments on this page](#) | [RSS feed for all comments](#)